Determination of the Ternary Modular Groups.

BY LEONARD EUGENE DICKSON.*

---

1. The determination of all groups of linear homogeneous transformations on m variables with coefficients in the $GF[p^n]$ falls naturally into two cases: (i) order a multiple of p; (ii) order prime to p. In the second case, the canonical form of any transformation merely multiplies each variable by a constant, and the problem is analogous to that of the determination of the finite groups of collineations in m variables.† This separation of cases was followed in the treatment of binary groups.‡

In his elaborate memoir on ternary groups, Burnside ‖ makes the limitation that $p^2 + p + 1$ shall be the product of at most two prime factors > 3 or else the triple of such a product. His discussion is occasionally incorrect. In particular, he misses** the groups with an invariant ternary quadratic form.

The present paper on the ternary groups of order a multiple of p employs methods entirely different from those used by Burnside. There is no limitation on the odd prime p. Moreover, a representative of each set of conjugate subgroups is exhibited in explict form.

2. The order of the group G of all ternary transformations modulo p of determinant unity is $p^3(p^3-1)(p^2-1)$. Every subgroup of order a power of

---

* Research Assistant to the Carnegie Institution of Washington.

† References to the work of Klein, Gordan, Jordan, and Valentiner are given in the new attack by Blichfeldt, Transactions, Vol. 4, p. 387; Vol. 5, p. 310.

‡ Compare the related problem of the unary linear fractional group treated by Moore, Burnside, Wiman, and Dickson (references in Linear Groups, p. 260). The writer has recently made a complete determination of the binary groups of determinant unity in the $GF[p^n]$.

‖ Proc. Lond. Math. Soc., Vol. XXVI, pp. 58-106.

§ Ibid., pp. 77, 81, 102-104. Cf. Amer. Journ. Math., Vol. XXII (1900), p. 231.

** Burnside, ibid., p. 81.

p is, therefore, conjugate with a subgroup of the group G_{p^3} of the operators

$$\begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix}. \tag{1}$$

In case a subgroup of G_{p^3} is defined by certain independent relations $r_1=0, \ldots, r_s=0$ between a, b, c, we denote it $\{r_1=0, \ldots, r_s=0\}$. We employ also the usual notation

$$B_{i,j,\lambda}: \quad \xi_i' = \xi_i + \lambda\xi_j, \quad \xi_k' = \xi_k, \qquad (k \neq i). \tag{2}$$

Since the commutator subgroup of G_{p^3} is formed of the operators $B_{3,1,\delta}$, and since the p^{th} power of (1) is of the form $B_{3,1,\delta}$, it follows that G_{p^3} has exactly $p+1$ subgroups of order p^2. But any linear relation between a and c defines such a subgroup. *Hence* the subgroups of order p^2 of G_{p^3} are $\{a=0\}$ and $\{c=ta\}$, $t=0, 1, \ldots, p-1$.*

The $p+1$ subgroups C_p of $\{a=0\}$ are $\{a=c=0\}$, $\{a=0,\ b=wc\}$, $w=0, 1, \ldots, p-1$. Now $B_{2,1,w}$ transforms the latter into $\{a=b=0\}$. The $p+1$ subgroups C_p of $\{c=ta\}$ are $\{a=c=0\}$, $\{c=ta,\ b=\frac{1}{2}ta^2+va\}$. When the latter is transformed by $B_{3,2,s}$, the only change is the replacement of v by $v+s$. We may thus make $v=0$. *Within G every subgroup of order p is conjugate with $(B_{3,2,1})$ or $J_t \equiv \{c=ta,\ b=\frac{1}{2}ta^2\}$, $t \neq 0$.*

3. The conditions for $\{c=ta\}(\alpha_{ij})=(\alpha_{ij})\{C=sA\}$ are

$$\alpha_{12}=\alpha_{13}=s\alpha_{23}=t\alpha_{23}=0, \quad ta\alpha_{33}=sA\alpha_{22}, \tag{3}$$

$$a\alpha_{22}+b\alpha_{23}=A\alpha_{11}, \quad a\alpha_{32}+b\alpha_{33}=B\alpha_{11}+sA\alpha_{21}. \tag{4}$$

Since $|\alpha_{ij}| \neq 0$, t and s are both zero or both $\neq 0$. For $t=s=0$, the conditions reduce to $\alpha_{12}=\alpha_{13}=0$, since (4) serve to determine A and B in terms of a and b, or vice versa. For $t \neq 0$, $s \neq 0$, then $\alpha_{23}=0$, $A=a\alpha_{22}\alpha_{11}^{-1}$ by $(4)_1$, and $t\alpha_{33}=s\alpha_{22}^2\alpha_{11}^{-1}$ by the final condition (3). Now $|\alpha_{ij}|=\alpha_{11}\alpha_{22}\alpha_{33}=1$. Hence $t=s\alpha_{22}^3$. Let d be the greatest common divisor of 3 and $p-1$. If $d=1$, every integer is a cubic reside modulo p, so that $t=s\alpha_{22}^3$ can always be satisfied. If $d=3$, the two groups are conjugate if, and only if, t/s is a root of $y^{\frac{1}{3}(p-1)} \equiv 1 \pmod{p}$. *If $p=3$ or if $p=3l-1$, the groups $\{c=ta\}$, $t=1, \ldots, p-1$, are all conjugate within G; if $p=3l+1$, they fall into three sets represented by $t=1, \beta, \beta^2$,*

* Cf. Bulletin, Vol. X (1904), p. 392, formula (9).

where β is a particular non-cubic residue of p. For any p, $\{c=ta\}$, $t\neq 0$, is commutative with only the operators $(5)_1$, with $\alpha_{22}^3=1$; $\{c=0\}$ with only $(5)_2$; $\{a=0\}$ with only $(5)_3$; G_{p^3} with only $(5)_1$, the determinant to be unity in each case:

$$\begin{pmatrix}\alpha_{11} & 0 & 0\\ \alpha_{21} & \alpha_{22} & 0\\ \alpha_{31} & \alpha_{32} & \alpha_{33}\end{pmatrix},\quad \begin{pmatrix}\alpha_{11} & 0 & 0\\ \alpha_{21} & \alpha_{22} & \alpha_{23}\\ \alpha_{31} & \alpha_{32} & \alpha_{33}\end{pmatrix},\quad \begin{pmatrix}\alpha_{11} & \alpha_{12} & 0\\ \alpha_{21} & \alpha_{22} & 0\\ \alpha_{31} & \alpha_{32} & \alpha_{33}\end{pmatrix}. \tag{5}$$

By a similar proof, *there are exactly d non-conjugate sets of cyclic $J_t\equiv\{c=ta,\ b=\frac{1}{2}ta^2\}$, $t\neq 0$; J_t is commutative with only the operators $(5)_1$ with $\alpha_{22}^2=\alpha_{11}\alpha_{33}$, $\alpha_{22}^3=1$, $\alpha_{32}=t\alpha_{33}\alpha_{21}\alpha_{22}^{-1}$. Also, $(B_{3,2,1})$ is commutative with only the operators $(5)_3$ with $\alpha_{21}=0$, $\alpha_{11}\alpha_{22}\alpha_{33}=1$.*

4. Lemma. *The only factors $\equiv 1\pmod{p^2}$ of $(p^3-1)(p^2-1)=\omega$ are* 1, ω.

Let $\omega=(1+p^2x)q$, $x>0$. Then $q\equiv 1\pmod{p^2}$, $q=1+p^2y$, $y\overline{\gtrless}0$. Then $p^3-p-1=x+y+p^2xy$. Hence

$$x+y=tp^2-p-1,\quad xy=p-t,\qquad t>0.$$

Now $y=0$ gives $1+p^2x=\omega$. Next, for $y\overline{\gtrless}1$, $x\overline{\gtrless}1$, the second condition requires that x and y be each $<p$. By the first, $tp^2-p-1\overline{\gtrless}2p-2$. But $p^2-3p+1>0$ if $p\overline{\gtrless}3$. For $p=2$, the lemma is evidently true.

5. Lemma. *Any binary transformation $B=\begin{pmatrix}\alpha & \gamma\\ \beta & \delta\end{pmatrix}$, $\gamma\neq 0$, and all the $E_\lambda=\begin{pmatrix}1 & 0\\ \lambda & 1\end{pmatrix}$ generate every binary transformation T of determinant unity.*

Indeed,

$$E_{-\alpha\gamma^{-1}}BE_{-\delta\gamma^{-1}}=\begin{pmatrix}0 & \gamma\\ \tau & 0\end{pmatrix},\quad \tau=-\gamma^{-1}(\alpha\delta-\beta\gamma)\neq 0.$$

The latter transforms E_λ into $F_\sigma=\begin{pmatrix}1 & \sigma\\ 0 & 1\end{pmatrix}$, where $\sigma=\lambda\gamma\tau^{-1}$ may be made arbitrary. But the E_λ and F_σ are known to generate every T.

6. Let H be a subgroup of order p^3N, normalized to contain G_{p^3}. If the latter is self-conjugate, the operators of H are (§3) all of the form $(5)_1$, so that H is given by the extension of G_{p^3} by certain operators

$$M_{\alpha,\beta,\gamma}:\ \xi_1'=\alpha\xi_1,\quad \xi_2'=\beta\xi_2,\quad \xi_3'=\gamma\xi_3,\quad \alpha\beta\gamma\equiv 1.$$

Next, let H contain $k > 1$ groups conjugate with G_{p^3}. Unless $H = G$, $k \neq 1 \pmod{p^2}$ by §4. Hence* G_{p^3} and one of its conjugates under H have a common subgroup of order p^2. Hence† H has an operator S commutative with this G_{p^2} but not with G_{p^3}.

(i). Let first G_{p^2} be $\{a = 0\}$. Then S is of the form $(5)_3$ with $\alpha_{12} \neq 0$. By choice of α and β, $B_{3,1,\alpha} B_{3,2,\beta} S$ has $\alpha_{31} = \alpha_{32} = 0$, $\alpha_{12} \neq 0$. Hence (§5) H contains every binary transformation B of determinant unity on ξ_1, ξ_2. *If H contains an operator $\Sigma = (\beta_{ij})$, β_{13} and β_{23} not both zero, then $H = G$.* Indeed, applying $\xi_1' = \xi_2$, $\xi_2' = -\xi_1$ on the right of Σ if necessary, we may set $\beta_{13} \neq 0$. Applying $M_{\beta_{13}^{-1},\, \beta_{13},\, 1}$ on the right, we reach Σ_1 with $\beta_{13} = 1$. Then

$$\Sigma_1 B_{2,1,-\beta_{23}} B_{3,1,-\beta_{33}} = (\gamma_{ij}), \quad \gamma_{13} = 1, \ \gamma_{23} = \gamma_{33} = 0, \ \begin{vmatrix} \gamma_{21} & \gamma_{22} \\ \gamma_{31} & \gamma_{32} \end{vmatrix} = 1.$$

Multiplying on the right by the inverse of $\begin{pmatrix} \gamma_{21} & \gamma_{22} \\ \gamma_{31} & \gamma_{32} \end{pmatrix}$ on ξ_1 and ξ_2, and then on the left by $B_{3,1,-\gamma_{11}} B_{3,2,-\gamma_{12}}$, we obtain $(\xi_1 \xi_3 \xi_2)$. This transforms $B_{3,2,\rho}$ and $B_{1,2,\rho}$ into $B_{1,3,\rho}$ and $B_{2,3,\rho}$, respectively. But all the $B_{i,j,\rho}$ generate G.

(ii). Let next G_{p^2} be $\{c = 0\}$. Then S is of the form $(5)_2$ with $\alpha_{23} \neq 0$. By choice of a and b, $SB_{2,1,a}B_{3,1,b}$, has $\alpha_{21} = \alpha_{31} = 0, \alpha_{23} \neq 0$. Then (§5), H contains every binary transformation on ξ_2, ξ_3 of determinant 1. If H contains an operator not of the form $(5)_2$, then $H = G$; the proof is quite similar to that in case (i).

(iii). Let finally G_{p^2} be $\{c = ta\}$, $t \neq 0$. Every operator commutative with it is of the form $(5)_1$ and hence is commutative with G_{p^3}.

THEOREM.—*Within G every subgroup of order a multiple of p^3 is conjugate with one of the following*: (i) *the group of all the p^3fg operators* $(5)_1$ *with* $\alpha_{11}^f = 1$, $\alpha_{22}^g = 1$, $\alpha_{33} = \alpha_{11}^{-1}\alpha_{22}^{-1}$; (ii) *the group of all the $fp^3(p^2-1)$ operators* $(5)_2$ *with* $\alpha_{11}^f = 1$, $\alpha_{22}\alpha_{33} - \alpha_{23}\alpha_{32} = \alpha_{11}^{-1}$; (iii) *the group of all the $fp^3(p^2-1)$ operators* $(5)_3$ *with* $\alpha_{33}^f = 1$, $\alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21} = \alpha_{33}^{-1}$. *Here f and g may be any divisors of $p - 1$.*

7. Let H be a subgroup of order p^2N, normalized to contain a subgroup of order p^2 of G_{p^3}. We prove that this G_{p^2} must be self-conjugate under H. If the number of conjugates to G_{p^2} is ω, H is of index p under G, whereas the order

---

*Cf. Burnside's Theory of Groups, p. 94, Cor. II.

† Ibid., p. 97.

of the simple linear fractional group $LF(3, p)$ does not divide $p!$. Hence (§4) G_{p^2} and one of its conjugates under H have a common cyclic C_p, and H has an operator commutative with C_p but not with G_{p^2}. By §3, this is impossible if C_p is J_t or $(B_{3,2,1})$, since, in the latter case, G_{p^2} must be $\{a=0\}$.

The quotient of the group of the operators $(5)_2$ by $\{c=0\}$ may be taken concretely as the group of the operators $(5)_2$ with $\alpha_{21}=\alpha_{31}=0$. We must take a group of the latter operators of period prime to p. The corresponding group of binary operators of determinant 1 on ξ_2 and ξ_3 must have the order 1, 2, $4k$, 24, 48 or 120 (see third foot-note to § 1).

The quotient of the group of the operators $(5)_1$ with $\alpha_{22}^3=1$ by $\{c=ta\}$ may be taken concretely as the group Q of the products $R_{\alpha,\rho}M_\epsilon$,

$$R_{\alpha,\rho}=\begin{pmatrix}\rho^{-1} & 0 & 0\\ 0 & 1 & 0\\ 0 & \alpha & \rho\end{pmatrix},\quad M_\epsilon=\begin{pmatrix}\varepsilon & 0 & 0\\ 0 & \varepsilon & 0\\ 0 & 0 & \varepsilon\end{pmatrix},\quad \varepsilon^d=1.$$

Within Q any subgroup of order prime to p is conjugate a group of operators $R_{0,\rho}M_\epsilon$.

THEOREM.—*Every subgroup H of order a multiple of p^2 but not of p^3 contains a self-conjugate G_{p^2}. Within G, H is conjugate with a group of operators $(5)_1$ with*

$$\alpha_{22}^3=1,\quad \alpha_{11}\alpha_{22}\alpha_{33}=1,\quad \alpha_{32}=t\alpha_{21}\alpha_{33}\alpha_{22}^{-1},$$

where t is a constant having one of d values; or a group of operators $(5)_2$ in which the $\begin{pmatrix}\alpha_{22} & \alpha_{23}\\ \alpha_{32} & \alpha_{33}\end{pmatrix}$ define a binary group of order prime to p; or a group of operators $(5)_3$ with an analogous restriction.

8. Let H be a subgroup of order pN, normalized to contain $(B_{3,2,1})$. Suppose, first, that the latter is self-conjugate. The quotient-group Q of the group of operators $(5)_3$ with $\alpha_{21}=0$ by $(B_{3,2,1})$ may be taken concretely as the group of the $p^2(p-1)^2$ operators $(5)_3$ with $\alpha_{21}=\alpha_{31}=0$, $\alpha_{11}\alpha_{22}\alpha_{33}=1$. Q contains self-conjugately the group of the p^2 operators $(6)_1$:

$$\begin{pmatrix}1 & \beta & 0\\ 0 & 1 & 0\\ 0 & \gamma & 1\end{pmatrix},\quad \begin{pmatrix}\alpha_{11} & \beta(\alpha_{22}-\alpha_{11}) & 0\\ 0 & \alpha_{22} & 0\\ 0 & \gamma(\alpha_{22}-\alpha_{33}) & \alpha_{33}\end{pmatrix}. \qquad (6)$$

Now $(6)_1$ transforms $M_{\alpha_{11}, \alpha_{22}, \alpha_{33}}$ into $(6)_2$. Hence Q contains p^2 subgroups of order $(p-1)^2$, no two of which have a common operator other than $M_{\epsilon, \epsilon, \epsilon}$, $\epsilon^d = 1$. The remaining dp^2 operators in Q are products of the form $(6)_1\, M_{\epsilon, \epsilon, \epsilon}$. Hence, every subgroup of order prime to p of Q is conjugate within Q with a group of operators $M_{\alpha, \beta, \gamma}$. Hence H is conjugate with the first group of the theorem below.

Let next $(B_{3,2,1})$ be not self-conjugate in H, which, therefore, contains an operator $S = (\alpha_{ij})$ with α_{13}, α_{23}, α_{21} not all zero (§3). We simplify S by transforming it by operators M, $B_{1,2,\rho}$ and $B_{3,1,\rho}$, each commutative with $(B_{3,2,1})$, and by multiplying it on the right or left by $B_{3,2,\rho}$. Now, any (α_{ij}) transforms $B_{3,2,1}$ into

$$\xi_i' = \xi_i + \alpha_{i3}\eta, \qquad (i = 1, 2, 3), \tag{7}$$

where η is the function by which $(\alpha_{ij})^{-1}$ replaces ξ_2.

(i). Let $\alpha_{23} \neq 0$. Transforming S by $M_{\alpha_{23}^{-1}, 1, \alpha_{23}}$, we may set $\alpha_{23} = 1$. Transforming by $B_{1,2,-\alpha_{13}}$, we have $\alpha_{13} = 0$. Then $SB_{3,2,-\alpha_{33}}$ has $\alpha_{23} = 1$, $\alpha_{13} = \alpha_{33} = 0$. Then (7) becomes

$$\xi_1' = \xi_1, \quad \xi_2' = \alpha_{31}\xi_1 + \xi_2 - \alpha_{11}\xi_3, \quad \xi_3' = \xi_3, \qquad (\alpha_{11}, \alpha_{31} \text{ not both } 0). \tag{8}$$

If $\alpha_{11} = 0$, we reach $B_{2,1,1}$, whereas the order of H is not divisible by p^2. Hence $\alpha_{11} \neq 0$, and $B_{3,1,-\alpha_{31}\alpha_{11}^{-1}}$ transforms (8) into $B_{2,3,-\alpha_{11}}$. Hence H contains all binary transformations B of determinant unity on ξ_2, ξ_3.

(ii). Let $\alpha_{23} = 0$, $\alpha_{13} \neq 0$. Transforming by $M_{\alpha, \beta, \gamma}$ and $B_{3,1,\rho}$, we may set $\alpha_{13} = 1$, $\alpha_{33} = 0$. Then (7) becomes

$$S_1: \quad \xi_1' = \xi_1 - \alpha_{31}\xi_2 + \alpha_{21}\xi_3, \quad \xi_2' = \xi_2, \quad \xi_3' = \xi_3.$$

For $\alpha_{21} = 0$, S_1 and $B_{3,2,1}$ generate a G_{p^2}. For $\alpha_{21} \neq 0$,

$$S_1^{-1}\, B_{3,2,\rho}^{-1}\, S_1\, B_{3,2,\rho} = B_{1,2,-\rho\alpha_{21}}.$$

But this and S_1 generate a G_{p^2}.

(iii). Let $\alpha_{23} = \alpha_{13} = 0$, $\alpha_{21} \neq 0$, whence $\alpha_{33} \neq 0$. Then (7) becomes

$$\xi_1' = \xi_1, \ \xi_2' = \xi_2, \ \xi_3' = -\alpha_{21}\alpha_{33}^2\xi_1 + \alpha_{11}\alpha_{33}^2\xi_2 + \xi_3.$$

But this and $B_{3,2,1}$ generate a G_{p^2}.

It remains only to discuss the groups of case (i). Suppose that H contains (β_{ij}) with β_{12}, β_{13}, β_{21}, β_{31} not all zero.

If $\beta_{12}=\beta_{13}=0$, we apply a B on the right and make also $\beta_{23}=\beta_{32}=0$, $\beta_{33}=1$, whence $\beta_{22}=\beta_{11}^{-1}$. If $\beta_{21}=0$, so that $\beta_{31}\neq 0$,

$$(\beta_{ij})^{-1}\, M_{1,-1,-1}^{-1}\, (\beta_{ij})\, M_{1,-1,-1}=B_{3,1,-2\beta_{31}\beta_{11}^{-1}},$$

and H contains a G_{p^2}. The case $\beta_{21}\neq 0$ is excluded by (iii).

Hence β_{12} and β_{13} are not both zero. Applying a B on the left, we may set $\beta_{12}=1$, $\beta_{13}=0$. Applying next a B on the right, we may set also $\beta_{23}=0$, $\beta_{33}=1$. The case $\beta_{21}\neq 0$ is excluded by (iii). Hence $\beta_{21}=0$, $\beta_{22}=\beta_{11}^{-1}$. Applying $B_{3,2,-\beta_{32}}$ on the left, we may set also $\beta_{32}=0$. Then

$$(\beta_{ij})^{-1}\, M_{1,\frac{1}{2},2}^{-1}\, (\beta_{ij})\, M_{1,\frac{1}{2},2}=\begin{pmatrix}1 & \beta_{11} & 0\\ 0 & 1 & 0\\ \beta_{11}^{-1}\beta_{31} & -\beta_{31} & 1\end{pmatrix}$$

is of period p and is commutative with $B_{3,2,1}$, so that the two generate a G_{p^2}. We have now proved the

THEOREM.—*According as a subgroup of order a multiple of p but not of p^2 contains $(B_{3,2,1})$ self-conjugately or not, it is conjugate within G with a group of pg products $B_{3,2,\rho}\, M_{\alpha,\beta,\alpha^{-1}\beta^{-1}}$, g a divisor of $(p-1)^2$, or with the group of order $pf(p^2-1)$ given by the extension of the binary group of determinant unity on ξ_2, ξ_3 by $M_{\alpha,\alpha^{-1},1}$, $\alpha^f\equiv 1$ (mod p.)*

9. Finally, let H be a subgroup of order pN, normalized within G to contain J_t. By section 3, any operator T commutative with J_t may be expressed as the product of $M_{\epsilon,\epsilon,\epsilon}$, $\varepsilon^d=1$, by

$$\begin{pmatrix}\rho^{-1} & 0 & 0\\ \alpha & 1 & 0\\ \beta & t\alpha\rho & \rho\end{pmatrix}=\begin{pmatrix}\rho^{-1} & 0 & 0\\ 0 & 1 & 0\\ \beta-\frac{1}{2}t\alpha^2\rho & 0 & \rho\end{pmatrix} S_{\alpha\rho},\quad S_a\equiv\begin{pmatrix}1 & 0 & 0\\ a & 1 & 0\\ \frac{1}{2}ta^2 & ta & 1\end{pmatrix},$$

where S_a is the general operator of J_t and $S_a=S_1^{a}$. The quotient group $Q=(T)\,/\,J_t$ may be taken concretely as the group of the $dp\,(p-1)$ products $M_{\epsilon,\epsilon,\epsilon}\, M_{\rho^{-1},1,\rho}\, B_{3,1,\gamma}$. Hence Q contains p groups conjugate with $(M_{\epsilon\rho^{-1},\epsilon,\epsilon\rho})$ ρ being a primitive root of p, no two of them have common operators other than $M_\epsilon\equiv M_{\epsilon,\epsilon,\epsilon}$. The remaining dp operators of Q lie in $(M_\epsilon,\, B_{3,1,\gamma})$. Within Q every subgroup of order prime to p is, therefore, conjugate with a subgroup of $(M_\epsilon,\, M_{\rho^{-1},1,\rho})$.

Let first J_t be self-conjugate in H. Then H is conjugate with a group of efp products $M_\epsilon\, M_{\sigma^{-1},1,\sigma}\, B_{3,1,\lambda}$.

Let next J_t be not self-conjugate in H. It suffices to consider the case $t=1$, since $M_{1,1,t^{-1}}$ transforms J_t into J_1, and H into a subgroup of G; the final list of the groups with J_1 must be transformed by the inverse $M_{1,1,t}$. Hence let H contain J_1 and an operator $S=(\alpha_{ij})$ with α_{12}, α_{13}, α_{23} not all zero (so that S shall not transform J_1 into a subgroup of G_{p^3}).

(i) Let $\alpha_{13}\neq 0$. Multiplying S on the left by an S_a, we may set $\alpha_{12}=0$. If then $\alpha_{22}=0$, S^{-1} has $\alpha'_{13}=0$, $\alpha'_{12}=\alpha_{13}\,\alpha_{32}\neq 0$, case (ii). Let now $\alpha_{22}\neq 0$. Then SS_a has $\alpha_{12}=\alpha_{32}=0$. Transforming by $B_{3,1,\sigma}$, which is commutative with S_a, we reach a transformation Σ with $\alpha_{12}=\alpha_{32}=\alpha_{33}=0$, $-\alpha_{13}\,\alpha_{31}\,\alpha_{22}=1$. The transform of S_a by Σ is

$$\begin{pmatrix} 1+a\alpha_{23}\alpha_{13}\alpha_{31} & -a\alpha_{13}^2\alpha_{31} & -a\alpha_{13}\left(D+\frac{1}{2}\,a\alpha_{22}\alpha_{13}\right) \\ a\alpha_{23}^2\alpha_{31} & 1-a\alpha_{23}\alpha_{31}\alpha_{13} & -aD\alpha_{23}-a\alpha_{22}^2\alpha_{13}-\frac{1}{2}\,a^2\alpha_{13}\alpha_{22}\alpha_{23} \\ 0 & 0 & 1 \end{pmatrix}, \tag{9}$$

where $D=\alpha_{11}\alpha_{23}-\alpha_{13}\alpha_{21}$. If $D\neq 0$, we can determine a to make $\alpha'_{12}\neq 0$, $\alpha'_{13}=0$, case (ii). If $D=0$, the transform of Σ^{-1} by $B_{3,1,\alpha_{11}\alpha_{13}^{-1}}$ is of the form Σ with $D'=-\alpha_{23}$; then $D'=0$ requires $\alpha_{23}=\alpha_{21}=0$. In the latter case, (9) becomes W_α if we take $a=-\alpha_{22}^{-2}\alpha_{13}^{-1}$, and set $\alpha=-\alpha_{22}^{-3}$:

$$W_\alpha=\begin{pmatrix} 1 & \alpha & \frac{1}{2}\alpha \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},\quad V=\begin{pmatrix} 0 & 0 & \frac{1}{2}\alpha \\ 2\alpha^{-1}(\alpha-1) & -1 & 1-\alpha \\ 2\alpha^{-1} & 0 & 0 \end{pmatrix}.$$

Applying the method by which S was reduced to Σ, we compute $S_{-2}W_\alpha S_{-2}$ and transform it by $B_{3,1,\sigma}$, where $\sigma=2\,(1-\alpha)\,\alpha^{-1}$. There results V, which is of the form Σ with $D=1-\alpha$. We are thus led to case (ii) unless $\alpha=1$. For $\alpha=1$, V becomes T, which transforms S_a into E_a:

$$T=\begin{pmatrix} 0 & 0 & \frac{1}{2} \\ 0 & -1 & 0 \\ 2 & 0 & 0 \end{pmatrix},\quad E_a=\begin{pmatrix} 1 & -\frac{1}{2}a & \frac{1}{8}a^2 \\ 0 & 1 & -\frac{1}{2}a \\ 0 & 0 & 1 \end{pmatrix}.$$

For brevity set $N_\rho=M_{\rho,1,\rho^{-1}}$. We have the relations

$$E_a=E_1^a,\quad S_a=S_1^a,\quad S_aN_\rho=N_\rho S_{a\rho^{-1}},\quad E_aN_\rho=N_\rho E_{a\rho}, \tag{10}$$

$$T^2=\text{identity},\quad TS_a=E_aT,\quad TN_\rho=N_{\rho^{-1}}T, \tag{11}$$

$$E_cS_b=N_{a^2c^{-2}}\,S_{-bca^{-1}}E_{-a},\qquad \left(a=\frac{4c}{bc-4},\ c\neq 0,\ b\neq\frac{4}{c}\right), \tag{12}$$

$$E_cS_{4c^{-1}}=N_{4c^{-2}}S_{-c}\,T,\qquad (c\neq 0). \tag{13}$$

Every operator of the group K generated by S_1 and T can be expressed in one of the two forms

$$N_{k^2}S_bE_a = \begin{pmatrix} k^2\left(1-\frac{ab}{4}\right)^2 & -\frac{a}{2}\left(1-\frac{ab}{4}\right) & \frac{1}{8}a^2k^{-2} \\ bk^2\left(1-\frac{ab}{4}\right) & 1-\frac{ab}{2} & -\frac{1}{2}ak^{-2} \\ \frac{1}{2}b^2k^2 & b & k^{-2} \end{pmatrix}, \qquad (14)$$

$$N_{k^2}S_bT = \begin{pmatrix} \frac{1}{4}b^2k^2 & \frac{1}{2}b & \frac{1}{2}k^{-2} \\ -bk^2 & -1 & 0 \\ 2k^2 & 0 & 0 \end{pmatrix}. \qquad (15)$$

First, S_1 times either reduces at once to one of these forms by (10). Next, by (11),

$$T\,.\,N_{k^2}S_bE_a = N_{k^{-2}}E_bS_aT, \qquad T\,.\,N_{k^2}S_bT = N_{k^{-2}}E_b.$$

For $a=0$, $N_{k^{-2}}E_bT = N_{k^{-2}}N_{4b^{-2}}S_{-b}E_{-4b^{-1}}$, of the form (14), the equality following from (13) upon transforming its members by T. For $a \neq 0$,

$$N_{k^{-2}}E_bS_aT = N_{k^{-2}}E_b\,.\,N_{a^2/4}E_{-a}S_{-4a^{-1}}, \quad \text{by (13)},$$
$$= N_{k^{-2}a^2/4}E_{-a+ba^2/4}S_{-4a^{-1}}, \quad \text{by } (10)_4,$$

and hence is of one of the forms (14), (15), in view of (12) and (13). Hence the group K is composed of the $\frac{1}{2}p(p^2-1)$ distinct operators (14) and (15). These may be combined into the simple form, with the invariant $\xi_2^2 - 2\xi_1\xi_3$:

$$\begin{pmatrix} \alpha^2 & \alpha\beta & \frac{1}{2}\beta^2 \\ 2\alpha\gamma & \alpha\delta+\beta\gamma & \beta\delta \\ 2\gamma^2 & 2\gamma\delta & \delta^2 \end{pmatrix}, \quad \alpha\delta-\beta\gamma = 1. \qquad (16)$$

Indeed, (14) is obtained by setting

$$\alpha = k\left(1-\frac{ab}{4}\right), \quad \beta = -\tfrac{1}{2}ak^{-1}, \quad \gamma = \tfrac{1}{2}bk, \quad \gamma = k^{-1};$$

while (15) is obtained by setting $\alpha = -\frac{1}{2}bk$, $\beta = -k^{-1}$, $\lambda = k$, $\delta = 0$. Now α, β, λ, δ and their negatives give the same operator (16). Further, there are exactly $p(p^2-1)$ sets of solutions of $\alpha\delta-\beta\gamma \equiv 1 \pmod{p}$. *Hence K is simply isomorphic with the group Γ of all unary linear fractional substitutions of determinant unity modulo p.**

---

* Since S_1 is not conjugate with $B_{3,2,1}$, there follows the known theorem that Γ is not representable as a binary homogeneous group of determinant 1.

If ν be a particular not-square, N_ν extends K to a group K' of order $p(p^2-1)$, composed of all ternary transformations of determinant unity leaving $\xi_2^2-2\xi_1\xi_3$ absolutely invariant. Indeed, N_ν transforms S_1 and T into $S_{\nu-1}$ and $N_{\nu-2}T$, respectively.

Consider a group H' which contains K' and a further operator $S=(\alpha_{ij})$. Now S, TS, ST, TST do not all have $\alpha_{13}=0$. We, therefore, assume that $\alpha_{13}\neq 0$ in S. By choice of b,ρ,a, $S_bSN_\rho S_a=R$ has $\alpha_{12}=\alpha_{23}=0$, $\alpha_{13}=1$. Then

$$\Sigma\equiv R^{-1}N_{-1}RN_{-1}=\begin{pmatrix}1 & 0 & 0\\ -2\alpha_{21}\alpha_{22}\alpha_{33} & 1-2\alpha_{21}\alpha_{32} & 2\alpha_{21}\alpha_{22}\\ 2\alpha_{21}\alpha_{32}\alpha_{33} & 2\alpha_{31}\alpha_{32}-2\alpha_{11}\alpha_{32}\alpha_{33} & 1-2\alpha_{21}\alpha_{32}\end{pmatrix}.$$

If $\alpha_{21}\alpha_{22}\neq 0$, a suitable product $S_bN_\sigma\Sigma S_a$ gives V:

$$V=\begin{pmatrix}1 & 0 & 0\\ \gamma & 0 & 1\\ \delta & -1 & 0\end{pmatrix},\quad V^{-1}N_\rho^{-1}VN_\rho=\begin{pmatrix}1 & 0 & 0\\ \gamma(\rho^{-1}-\rho) & \rho & 0\\ \delta(\rho^{-2}-\rho^{-1}) & 0 & \rho^{-1}\end{pmatrix}.$$

We may take $\rho^3\neq 1$. Then (§3) the latter operator transforms J_1 into another subgroup of G_{p^3}, so that H' would be of order a multiple of p^2. The same is true for Σ if $\alpha_{22}=0$. If $\alpha_{21}=0$, $\Sigma=B_{3,1,k}$, $k=2\alpha_{31}\alpha_{32}-2\alpha_{11}\alpha_{32}\alpha_{33}$. If $k\neq 0$, we obtain a G_{p^2}. Hence $k=0$. Now $\alpha_{11}\alpha_{22}\alpha_{33}-\alpha_{31}\alpha_{22}=1=|S|$. Hence $\alpha_{32}=0$, and

$$S=\begin{pmatrix}\alpha_{11} & 0 & 1\\ 0 & \alpha_{22} & 0\\ \alpha_{31} & 0 & \alpha_{33}\end{pmatrix},\quad TST=\begin{pmatrix}\alpha_{33} & 0 & \frac{1}{4}\alpha_{31}\\ 0 & \alpha_{22} & 0\\ 4 & 0 & \alpha_{11}\end{pmatrix},\quad \alpha_{22}(\alpha_{11}\alpha_{33}-\alpha_{31})=1.$$

If $\alpha_{31}=0$, $N_\sigma TST$ can be given the form W with $\delta\neq 0$:

$$W=\begin{pmatrix}1 & 0 & 0\\ 0 & \alpha & 0\\ \delta & 0 & \alpha^{-1}\end{pmatrix},\quad Z=\begin{pmatrix}\alpha'_{11} & 0 & \alpha'_{13}\\ 0 & 1 & 0\\ -4\alpha'_{13} & 0 & \alpha'_{33}\end{pmatrix}.$$

Then $N_\rho^{-1}W^{-1}N_\rho W=B_{3,1,l}$, $l=\delta(1-\rho^{-2})$. Hence $\alpha_{31}\neq 0$. Then $S^{-1}N_\rho TST$ gives Z, where

$$\alpha'_{11}=\alpha_{22}(\rho\alpha_{33}^2-\tfrac{1}{4}\rho^{-1}\alpha_{31}^2),\quad \alpha'_{13}=\tfrac{1}{4}\rho^{-1}\alpha_{11}\alpha_{22}\alpha_{31}-\rho\alpha_{22}\alpha_{33}.$$

If $\alpha_{33}\neq 0$, we take $\rho=\frac{1}{2}\alpha_{31}\alpha_{33}^{-1}$, whence $\alpha'_{11}=0$, $\alpha'_{13}=\frac{1}{2}$. Then TZ is of the form W with $\alpha=-1$ and hence transforms J_1 into another subgroup of G_{p^3}.

Hence $\alpha_{33}=0$. If $\alpha_{11}\neq 0$, $N_\rho TST$ is of the form S with $\alpha_{31}\neq 0$, $\alpha_{33}\neq 0$, previously excluded. Hence $\alpha_{11}=\alpha_{33}=0$ in S. Then

$$STN_2=M\alpha_{31},\ \alpha_{31}^{-1},\ 1.$$

If $\alpha_{31}^3\neq 1$, this transforms J_1 into another subgroup of G_{p^3}. We thus reach the extender $M_{\epsilon^2,\epsilon,1}=M_{\epsilon,\epsilon,\epsilon}M_{\epsilon,1,\epsilon^2}$, $\epsilon^3=1$. Now $M_{\epsilon,\epsilon,\epsilon}$ occurs in K' if, and only if, $\epsilon=1$. Hence H' is of order $dp(p^2-1)$ and leaves $\xi_2^2-2\xi_1\xi_3$ relatively invariant.

We now pass from case (i) to the study of the group H with an operator $S=(\alpha_{ij})$, $\alpha_{13}=0$, α_{12} and α_{23} not both zero. These properties of S are not altered when we make the normalization as at the beginning of the section, in view of which the largest subgroup G_{pwe} of H commutative with J_1 is composed of the products $M_{\epsilon,\epsilon,\epsilon}N_\rho S_a$, $\rho^w=1$, $\epsilon^e=1$, $\epsilon=1$ or d. We defer to §10 the case $w=1$, assuming $w>1$ here.

(ii) $\alpha_{13}=0$, $\alpha_{12}\neq 0$. Transforming H by $N_{\alpha_{12}}^{-1}$, we may set $\alpha_{12}=1$ in S. Replacing S by a suitable product S_aSS_b, we may set $\alpha_{11}=\alpha_{13}=\alpha_{22}=0$, $\alpha_{12}=1$. Then $S^{-1}N_\rho SN_\rho^{-1}$ becomes

$$\begin{pmatrix}\rho^{-1} & 0 & 0\\ (\rho^{-1}-\rho)\,\alpha_{21}\alpha_{23}\alpha_{32} & \rho^{-1}\alpha_{23}\alpha_{31}-\rho\alpha_{21}\alpha_{33} & (\rho-\rho^{-1})\,\alpha_{21}\alpha_{23}\\ \rho\alpha_{32}+\alpha_{21}\alpha_{32}\alpha_{33}-\rho^2\alpha_{31}\alpha_{32}\alpha_{23} & (1-\rho^2)\,\alpha_{31}\alpha_{33} & \rho^2\alpha_{31}\alpha_{23}-\alpha_{21}\alpha_{33}\end{pmatrix}. \tag{17}$$

If ρ may take the value -1, (17) multiplies ξ_1 and ξ_2 by -1 and replaces ξ_3 by $\xi_3-2\alpha_{32}\xi_1$. Hence it transforms S_1 into an operator $\neq S_a$ of G_{p^3}, whereas the order of H is not a multiple of p^2. Let then $\rho^2\neq 1$. If $\alpha_{21}\alpha_{23}\neq 0$, (17) falls under case (iii). If $\alpha_{23}=0$, so that $|S|=-\alpha_{21}\alpha_{33}=1$, (17) is commutative with J_1 if, and only if, (§3) $\rho^3=1$, $\alpha_{31}=0$; when these hold, $w=3$, so that $\alpha'_{31}=(\rho-1)\,\alpha_{32}$ in (17) is zero. In view of S^2 we may set $a_{21}=\epsilon$, $\epsilon^3=1$. Then

$$S=\begin{pmatrix}0 & 1 & 0\\ \epsilon & 0 & 0\\ 0 & 0 & -\epsilon^2\end{pmatrix},\quad S_{-\epsilon^2}S^{-1}S_{\epsilon^2}SN_{\epsilon^2}S_{-1}S=\begin{pmatrix}-\epsilon^2 & 0 & 0\\ 0 & \epsilon & 0\\ -\epsilon & 2\epsilon^2 & -1\end{pmatrix},$$

while the latter transforms J_1 into a different subgroup of G_{p^3} (§3). The remaining case $\alpha_{21}=0$ may be excluded in a similar way.

(iii) $\alpha_{13}=\alpha_{12}=0$, $\alpha_{23}\neq 0$. Transforming H by N, we may set $\alpha_{23}=1$. Multiplying right and left by the S_a, we may set also $\alpha_{22}=\alpha_{33}=0$, whence

$-\alpha_{11}\alpha_{32}=1$. Then $S^{-1}N_\rho S N_\rho^{-1}=L$ is

$$\begin{pmatrix}1 & 0 & 0\\ \beta & \rho^{-1} & 0\\ \gamma & 0 & \rho\end{pmatrix}, \quad \begin{matrix}\beta=(\rho^{-1}-\rho)\,\alpha_{21}\alpha_{32}\,,\\ \gamma=(\rho-\rho^2)\alpha_{31}\alpha_{32}\,.\end{matrix}$$

If either $\beta\neq 0$ or $\rho^3\neq 1$, L leads to a G_{p^2} (§3). Let, then, $\beta=0$, $\rho^3=1$, $\rho\neq 1$ whence $\alpha_{21}=0$. Then $N_\rho^{-1}LN_\rho L^{-1}=B_{3,1,t}$, $t=\gamma(1-\rho^{-1})$, leads to a G_{p^2} unless $\gamma=0$. Hence we may set also $\alpha_{31}=0$. In view of S^2, we may set $\alpha_{32}=\varepsilon$, $\varepsilon^3=1$, whence $\alpha_{11}=-\varepsilon^2$. Then S and $S_{-1}S^{-1}S_\varepsilon\, SS_{-1}$ are, respectively,

$$\begin{pmatrix}-\varepsilon^2 & 0 & 0\\ 0 & 0 & 1\\ 0 & \varepsilon & 0\end{pmatrix}, \quad \begin{pmatrix}1 & 0 & 0\\ -2 & 0 & 1\\ 1 & -1 & 0\end{pmatrix}.$$

The latter, taken as S, leads to an L with $\beta\neq 0$.

10. It remains to consider the case in which J_1 is commutative only with its operators and the $M_{\epsilon,\epsilon,\epsilon}$, with $\varepsilon^e=1$, $e=1$ or 3. Denote the order of H by pem. We pass to the quotient-group Q of G by $(M_{\epsilon,\epsilon,\epsilon})$. From H, we obtain H_1 of order pm. Hence H_1 contains exactly m operators of order prime to p. By the canonical form theory, Q contains cyclic subgroups of order $\frac{1}{d}\,(p^2+p+1)$ each commutative with just $\frac{3}{d}\,(p^2+p+1)$ operators. Let μ be the order of the largest subgroup C of one of these cyclic groups which lies in H_1. Then C is one of $pm\div\mu\lambda$ conjugates within H_1, where $\lambda=1$ or 3, and no two of them have a common operator $\neq I$. Hence they contain at least $pm\,(\mu-1)\div 3\mu$ operators $\neq I$. But if $p>3$, this number exceeds m if $\mu>1$, and hence $\mu\,\overline{\gtrless}\,3$. Hence, for $p>3$, there occur no operators $\neq I$ whose periods divide $\frac{1}{d}\,(p^2+p+1)$. The same is true for $p=3$, since then $d=1$, $\mu=13$, $\lambda=3$, so that there are exactly $m/13$ C_{13} in H_1. But $m=2^i.13$, $i\,\overline{\gtrless}\,4$, contrary to Sylow's theorem. Next, H_1 contains no operators of period τ, a divisor of $\frac{1}{d}(p^2-1)$ but not of $\frac{1}{d}\,(p-1)$. Indeed, the cyclic C_τ would be one of $pm\div\tau\varkappa$ conjugates, where $\varkappa=1$ or 2. Let C_τ have t operators of periods dividing $\frac{1}{d}\,(p-1)$, $\tau\,\overline{\gtrless}\,2t$. Then there are at least $\tau-t$ operators in any C_τ

occurring in none of its conjugates. But $(\tau - t)pm \div \tau\varkappa \overline{>} \frac{1}{2} pm/\varkappa > m$ if $p > 3$. The case $p = 3$ is immediately treated since the group of order $3 . 2^i, 1 \overline{<} i \overline{<} 4$ has 2^i conjugate C_3 and a self-conjugate G_{2^i}, whence $i = 2$ or 4. If $i = 2$ and the G_4 is cyclic, there occurs a self-conjugate operator O_2 and hence an O_6. For $i = 4$, G_{16} must contain an O_8, since 16 is the highest power of 2 dividing the order of $G \equiv Q$, which contains operators of period $\frac{1}{d}(p^2 - 1) = 8$. But for $\tau = 8$, $t = 2$, the general argument gives $6 . 3 . m \div 8\varkappa$, or more than m, distinct operators of periods 4 and 8.

We have shown that H_1 contains no operator of period a divisor > 1 of $q = \frac{1}{d}(p^2 + p + 1)$, or a divisor of $r = \frac{1}{d}(p^2 - 1)$ but not of $s = \frac{1}{d}(p - 1)$. The order of Q is $q(p+1)(p-1)^2p^3$. Now q is relatively prime to $p + 1$ Also $(p-1)^2 - dq = -3p$, while q is not divisible by 3; hence q and $(p-1)^2$ are relatively prime. Hence the order of H_1 divides $(p+1)(p-1)^2p$. Any factor other than 2 or 4 of $p + 1$ is prime to $(p-1)^2$ and hence to s. Hence the order of H_1 divides $w = 2^k(p-1)^2p$, $k = 2$ if $p = 4l + 1$, $k = 4$ if $p = 4l + 3$. The order must divide $w/2$; otherwise H_1 would contain a group of order the highest power of 2 dividing the order of Q, and hence an operator of period a power of 2 dividing r but not s. Hence the order H_1 divides $\nu = \varkappa(p-1)^2p$, $\varkappa = 1$ or 2 according as $p = 4l \pm 1$. But the only divisors $\equiv 1 \pmod{p}$ of $2(p-1)^2$ are 1, $(p-1)^2$, and if $p = 7$ also 8. But C_p is to be commutative with no further operators of H_1. If $p = 7$ and H_1 is of order 56, there would occur an abelian subgroup G_8 of type (1, 1, 1), whereas a simple discussion shows that no such G_8 lies in $LF(3, 7)$. Hence H_1 is of order $p(p-1)^2$. Now $(p-1)^2$ has no factor $\equiv 1 \pmod{p}$ other than itself and unity. Moreover, C_p is not self-conjugate. Hence* $(p-1)^2$ does not have two distinct prime factors. Hence $p - 1 = 2^a$. Then $d = 1$, $\frac{1}{2}(p+1)$ is odd. Hence H_1 contains a $G_{2^{2a}}$ self-conjugate in a subgroup $G_{2^{2a+1}}$ of order the highest power of 2 in $LF(3, p)$. The latter has operators of period $p^2 - 1$, and hence operators of period 2^{a+1}. Hence $G_{2^{2a}}$ has operators of period 2^a. But no operator of period p transforms into itself a cyclic C_{2^i} $(i \overline{<} a)$, since there is no ternary group of order $p2^i$ containing J_1. Hence there are at least p distinct conjugates C_{2^i} in H_1

---

* Frobenius, Berliner Sitzungsberichte, 1902, p. 459.

and hence at least $p2^{i-1}$ distinct O_i. But

$$p\sum_{i=1}^{a} 2^{i-1} = p(2^a - 1) = 2^{2a} - 1.$$

Hence H_1 contains exactly p conjugate C_{2^i} for $i = 1, \ldots, a$. If two of the C_{2^a} had a common subgroup C_{2^b}, $b > 0$, all the p C_{2^a} would contain C_{2^b}, which would then be self-conjugate in H_1, contrary to the above. Hence all the operators of $G_{2^{2a}}$ lie in p conjugate G_{2^a}. Suppose that exactly 2^c operators transform each of the p cyclic C_{2^i} into itself. Then there would be a self-conjugate G_{2^c} in H_1. Hence, by above, $c = 2a$, so that $G_{2^{2a}}$ is abelian of type (a, a). Hence there are only 3 operators of period 2, whence $p = 3$. For $p = 3$, $H_1 = H$ is simply isomorphic with the alternating group on 4 letters. Its four-group may be taken, by applying a suitable ternary transformation, to be generated by $M_{-1,-1,1}$ and B_+, where

$$B_{\pm} = \begin{pmatrix} 0 & \pm 1 & 0 \\ \pm 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad C = \begin{pmatrix} \alpha_{11} & \pm\alpha_{11} & \alpha_{13} \\ \mp\alpha_{11} & -\alpha_{11} & \pm\alpha_{13} \\ \alpha_{31} & \mp\alpha_{31} & 0 \end{pmatrix}, \quad 4\alpha_{11}\alpha_{13}\alpha_{31} \equiv 1.$$

We find that any ternary operator of determinant 1 which transforms $M_{-1,-1,1}$ into $B_{\pm}$, and the latter into $B_{\mp}$, must be of the form C. Every such C is of period 3 and leaves absolutely invariant

$$\xi_1^2 + \xi_2^2 - \xi_3^2 \equiv \xi_2^2 - 2(\xi_1 + \xi_3)(\xi_1 - \xi_3), \qquad (\text{mod } 3).$$

The resulting G_{12} generated by $M_{-1,-1,1}$, B_+, and any C, is, therefore, conjugate within G with the group of the operators (16).

THE UNIVERSITY OF CHICAGO, *October*, 1904.